REMARKS

Claims 1-25 were withdrawn from consideration. Claims 26-50 were rejected under 35 U.S.C. 102(e) as being anticipated by Hagerman (USP 6,973,568).

Hagerman describes a storage area network resistant to spoofing and replay attacks. Hagerman details authentication using a hash function. "Each port is provided with a hash function generator for providing and verifying an authentication code for frames transmitted over the storage area network, and a key table for providing a key to the hash function generator. The authentication code is generated by applying a hash function to the key and to at least an address portion of each frame. In each node, the key is selected from that node's key table according to address information of the frame." (Abstract) "Fibre Channel storage area network utilizes frames having time-of-transmission and authentication-code fields." (Column 3, Lines 23-24) "The Authentication code field 300 is filled with a hash function of at least a key value, the transmitted time field 302, the S—ID field 304, the D—ID field 306, and any association header field 308. The hash function that generates authentication code field 300 may also operate upon additional fields of the header and payload, security is enhanced by including the payload 310. It is preferable that the hash function be computed by hardware associated with each port, such as hash function generators 182, 184, 186, 188, 190, and 192 (FIG. 1). Software hash function generators may consume considerable compute resources. The key value used to compute the authentication code field 300 is extracted from a key table 170, 172, 174, 176, 178, and 180 associated with each port." (Column 5, Lines 15-28) "The authentication code is computed using the MD2 hashing algorithm." (Column 3, Lines 41-42)

"Each node that receives the transmitted frame recomputes the authentication code based upon a key selected from the table according to the S—ID of the frame header. The recomputed authentication code is compared to that in the frame, those frames having mismatched authentication codes are dropped." (Column 3, Lines 48-53)

Hagerman is believed to teach or suggest only conventional fibre channel security. "In conventional implementations, no security is provided in the initialization messages. The techniques of the present invention provide mechanisms for embedding security in the initialization messages to create an initialization sequence with security… techniques are also provided for authentication between non-adjacent entities." (Page 9, Line 28 – Page 10, Line 4)

Independent claim 26 recites "identifying a security control indicator in the frame." Claim 50 similarly recites "means for identifying that the frame has been secured." Claims 38 and 46 have been amended to recite "providing a security control indicator in the fibre channel frame, wherein the security control indicator specifies that the fibre channel frame is encrypted." The material the Examiner cites does not teach or suggest any security control indicator. The Examiner argues that an authentication code field is a security control indicator. The authentication code field in Hagerman is "filled with a hash function" used for authentication. By contrast, the security control indicator is not a hash field. The security control indicator is used to indicate whether a frame supports security so that either conventional frame processing or modified frame processing can be used.

"Any indicator showing that the frame is secure is referred to herein as a security control indicator. It should also be noted that this is distinct from the above mentioned security enable indicator, which is used during an initialization sequence to show whether a newly introduced node supports security. A frame that supports encryption and authentication is herein referred to as a secured frame. A frame that supports only authentication is herein referred to as an authentication secured frame. A frame that supports only encryption is herein referred to as an encryption secured frame." (Page 20, Line 3-10) Hagerman has no indicator showing whether a frame is secure. An authentication code is provided in every frame and thus Hagerman has no need to provide a security control indicator. Furthermore, even if the authentication code in Hagerman is interpreted broadly as a security control indicator, the authentication code does not to indicate any encryption support associated with the frame. Consequently, Hagerman teaches or suggest no security control indicator.

Independent claim 26 also recites "decrypting the first portion of the frame by using algorithm information contained in the entry in the security database." Independent claim 50 also recites "means to decrypt the eventually encrypted frame." The material the Examiner cites only describes calculating an authentication code. Calculating an authentication includes performing authentication or hashing operations that are distinct from performing decryption operations. Other independent claims also recite encrypting or decrypting using information associated with a security database. Hagerman does not teach or suggest encrypting or decrypting using any information associated with a security database.

In light of the above remarks relating to independent claims, the remaining dependent claims are believed allowable for at least the reasons noted above. Applicants believe that all pending claims are allowable and respectfully request a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,
BEYER WEAVER & THOMAS, LLP

Godfrey K. Kwan
Reg. No. 46,850

P.O. Box 70250
Oakland, CA 94612-0250
(510) 663-1100